

# Optimal cyclic codes with generalized Niho type zeroes and the weight distribution

Maosheng Xiong\* and Nian Li†

February 17, 2015

## Abstract

In this paper we extend the works [16, 38] further in two directions and compute the weight distribution of these cyclic codes under more relaxed conditions. It is interesting to note that many cyclic codes in the family are optimal and have only a few non-zero weights. Besides using similar ideas from [16, 38], we carry out some subtle manipulation of certain exponential sums.

**2010 Mathematics Subject Classification:** 11T71, 94B15, 11L03

**Keywords:** Cyclic codes, weight distribution, Vandermonde matrix, Niho exponent

## 1 Introduction

Cyclic codes are an important class of linear codes. Due to their desirable algebraic properties and efficient algorithms for encoding and decoding processes, cyclic codes have been widely used in many areas such as communication and data storage system. They can also be used to construct other interesting structures such as quantum codes [28], frequency hopping sequences [8] and so on.

Let  $p$  be a prime number,  $l \geq 1$ ,  $q = p^l$  and  $\text{GF}(q)$  be the finite field of order  $q$ . A cyclic code  $\mathcal{C}$  of length  $n$  over  $\text{GF}(q)$  (assume  $(n, q) = 1$ ), by the one-to-one correspondence

$$\begin{aligned} \sigma : \quad \mathcal{C} &\rightarrow R := \text{GF}(q)[x]/(x^n - 1) \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}, \end{aligned}$$

can be identified with an ideal of  $R$ . There exists a unique monic polynomial  $g(x)$  with least degree such that  $\sigma(\mathcal{C}) = g(x)R$  and  $g(x) \mid (x^n - 1)$ . The  $g(x)$  is called the *generator polynomial* and  $h(x) := (x^n - 1)/g(x)$  is called the *parity-check polynomial* of  $\mathcal{C}$ . If  $h(x)$  has  $t$  irreducible factors over  $\text{GF}(q)$ , we follow the literature and say that “the dual of  $\mathcal{C}$  has  $t$  zeroes”. (Note that this is different from [38] in which we call “ $\mathcal{C}$  has  $t$  zeroes” instead.)  $\mathcal{C}$  is called *irreducible* if  $t = 1$  and *reducible* if  $t \geq 2$ .

Denote by  $A_i$  the number of codewords of  $\mathcal{C}$  with Hamming weight  $i$ , where  $0 \leq i \leq n$ . The study of the weight distribution  $(A_0, A_1, \dots, A_n)$  or equivalently the weight enumerator  $1 + A_1Y + A_2Y^2 + \dots + A_nY^n$  is important in both theory and application, because the weight

---

\*Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: mamsxiong@ust.hk).

†Department of Informatics, University of Bergen, 5020 Bergen, Norway (e-mail: nianli.2010@gmail.com).

distribution gives the minimum distance and thus the error correcting capability of the code, and the weight distribution allows the computation of the probability of error detection and correction with respect to some algorithms [14]. Moreover, the weight distribution is related to interesting and challenging problems in number theory ([4, 27]).

In a recent paper [16], the authors constructed some classes of cyclic codes whose duals have two Niho type zeroes and obtained the weight distribution. These classes of cyclic codes are quite interesting because they contain some optimal cyclic codes (among linear codes) and in general have only three or four non-zero weights. This beautiful work was recently extended to more general classes of cyclic codes whose duals may have arbitrary number of Niho type zeroes (see [38]). The purpose of this paper is to extend these works in yet two other directions. It is interesting to note that this not only vastly generalizes the construction of [16, 38], but also yields many optimal or almost optimal cyclic codes with very few non-zero weights, none of which was present in [16, 38] (See Examples 1–4, Tables 2 and 5 in Section 2). We study the weight distribution of these cyclic codes, by employing similar ideas from [16, 38] and by carrying out some quite subtle analysis of certain exponential sums.

In recent years, for many families of cyclic codes the weight distribution problem has been solved. We only mention here that most of the results are for cyclic codes whose duals have no more than three zeroes (see for example [1, 2, 3, 12, 21, 25, 26, 29, 30, 31, 34, 7] and [6, 9, 10, 11, 13, 17, 18, 19, 20, 22, 23, 32, 33, 35, 36, 37, 41]). There are only a few results for cyclic codes whose duals may have arbitrary number of zeroes ([15, 39, 40, 38]). The duals of the cyclic codes considered in this paper may also have arbitrary number of zeroes.

The paper is organized as follows. In Section 2, for any prime  $p$ , we introduce the cyclic codes  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  and  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  and the main results (Theorems 1 and 3). The special cases of 3-weight and 4-weight cyclic codes are presented in Corollaries 2 and 4. Then we provide numerical examples of optimal or almost optimal cyclic codes over GF(4) and GF(8) and compute the weight distribution. We also compile a list of such codes over other finite fields. In Section 3 we prove a simple lemma which will be used later. For  $p = 2$ , Statements (i) of Theorems 1 and 3 are proved in Section 4, and Statements (ii) of Theorems 1 and 3 are proved in Section 5. For  $p \geq 3$ , Statements (i) and (ii) of Theorems 1,3 are proved in Sections 6 and 7 respectively. As was noted in [16, 38], we remark here that the proofs for  $p = 2$  and  $p \geq 3$  are quite different. In Section 8 we conclude the paper.

## 2 Cyclic codes $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$ and $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$

From what follows, let  $p$  be a prime number, and  $l, m$  be positive integers. Let  $q = p^l$  and  $r = q^m$ . Denote by  $\text{GF}(r^2)$  the finite field of order  $r^2$ . Let  $\gamma$  be a primitive element of  $\text{GF}(r^2)$ .

### 2.1 Cyclic code $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$

For any integers  $h, f$ , define

$$e = (h, r + 1), \quad \delta = ((r + 1)f, (r - 1)e), \quad n = (r^2 - 1)/\delta. \quad (1)$$

Let  $t$  be an integer and assume that

$$(a). \quad 1 \leq t < \frac{r+1}{2e},$$

$$(b). \quad \left( f, \frac{r-1}{q-1} \right) = 1,$$

(c). if  $p$  is odd, then  $m$  is odd, or  $m$  and  $h$  are both even.

Let  $d_0, d_1, \dots, d_t$  be integers such that

$$d_j \equiv (jh + f)(r - 1) + 2f \pmod{r^2 - 1}, \quad 0 \leq j \leq t. \quad (2)$$

A positive integer  $d$  is called a *Niho exponent* if  $d \equiv q^j \pmod{r - 1}$  for some  $j$ . The Niho exponents were originally introduced by Niho [24] who investigated the cross-correlation between an  $m$ -sequence and its decimation. Since then, Niho exponents were further studied and had been used in other research topics. Here  $d_j \equiv 2f \pmod{r - 1} \forall j$  and  $\left( f, \frac{r-1}{q-1} \right) = 1$ , the  $d_j$ 's are called the “generalized Niho exponents”, and the  $\gamma^{-d_j}$ 's are called the “generalized Niho type zeroes”.

It can be seen that  $(d_0, d_1, \dots, d_t, r^2 - 1) = \delta$ . The  $q$ -ary cyclic code  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  of length  $n$  consists of elements  $c(\underline{a})$  given by

$$c(\underline{a}) = \left( \text{Tr}_{r/q}(a_0 \gamma^{d_0 i}) + \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j \gamma^{d_j i} \right) \right)_{i=0}^{n-1}, \quad (3)$$

where  $\underline{a} = (a_0, a_1, \dots, a_t)$  for any  $a_1, \dots, a_t \in \text{GF}(r^2)$  and  $a_0 \in \text{GF}(r)$ . Here  $\text{Tr}_{r/q}$  and  $\text{Tr}_{r^2/q}$  denote the trace map from  $\text{GF}(r)$  and  $\text{GF}(r^2)$  to  $\text{GF}(q)$  respectively. It will be seen that the dimension of  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  is always  $(2t + 1)m$  and the dual of  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  has the  $(t + 1)$  zeroes  $\gamma^{-d_0}, \dots, \gamma^{-d_t}$ .

We remark that a similar  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  over  $\text{GF}(p)$  was constructed in [38], but it required  $(2f, r - 1) = 1$ , which is valid only when  $p = 2$ . Here we consider  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  over  $\text{GF}(q)$  for any  $p$  under more flexible conditions. Note that (b) reduces to  $(2f, r - 1) = 1$  only if  $q = p = 2$ . As it turns out, the weight distribution of the new  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  is very similar to that in [38]. However, the proofs are much more involved. For the sake of completeness, we describe the weight distribution as follows.

Let  $N_0 = 1, N_1 = 0$  and define

$$N_k := k! e^k \sum_{\substack{\lambda_2, \lambda_3, \dots, \\ \sum_{j \geq 2} j \lambda_j = k}} \binom{\frac{r+1}{e}}{\sum_j \lambda_j} \left( \sum_j \lambda_j \right)! \prod_j \frac{(B_j/j!)^{\lambda_j}}{(\lambda_j)!}, \quad \forall k \geq 2. \quad (4)$$

Here the summation is over all non-negative integers  $\lambda_2, \lambda_3, \dots$  such that  $\sum_{j \geq 2} j \lambda_j = k$  and

$$B_j := r^{-1}(r - 1)^j + (-1)^j(1 - r^{-1}),$$

and  $\binom{u}{v}$  is the standard binomial coefficient “ $u$ -choose- $v$ ”. It is easy to compute that  $N_2 = e(r^2 - 1)$ ,  $N_3 = e^2(r - 2)(r^2 - 1)$ ,  $N_4 = e^2(r^2 - 1) \{(e + 3)r^2 - 6er + 6e - 3\}$ , etc. We prove the following.

**Theorem 1.** (i). For  $p = 2$  or  $p$  being an odd prime, under assumptions (1)–(3) and (a)–(c), the code  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  is a  $q$ -ary cyclic code of length  $n = (r^2 - 1)/\delta$  and dimension  $(2t + 1)m$ , with at most  $(2t + 1)$  non-zero weights, each of which is given by

$$w_j = \frac{q - 1}{q\delta} \cdot (r^2 - (je - 1)r), \quad 0 \leq j \leq 2t. \quad (5)$$

(ii). Let  $\mu_j$  be the frequency of the weight  $w_j$  for each  $j$ . Define  $\underline{\mu} = (\mu_0, \mu_1, \dots, \mu_{2t})^T$ , and  $\underline{b} = (b_0, b_1, \dots, b_{2t})^T$  where  $b_i = r^{2t+1}N_i - (r^2 - 1)^i$ . Then

$$\underline{\mu} = \left( M_t^{(1)} \right)^{-1} \underline{b}.$$

Here  $M_t^{(1)} = [m_{ij}]_{0 \leq i,j \leq 2t}$  is an invertible Vandermonde matrix whose entry is given by  $m_{ij} = (jer - r - 1)^i$ .

By using computer algebra such as **Mathematica**, Theorem 1 can be used easily to compute the weight distribution of  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  explicitly for any  $t$ , though the results are quite complicated to be written down even for  $t = 2$ . When  $t = 1$  which is the most interesting, it is a 3-weight cyclic code, whose weight distribution can be described as follows.

**Corollary 2.** Under assumptions (1)–(3) and (a)–(c) for  $t = 1$ , the code  $\mathcal{C}_{(d_0, d_1)}^{(1)}$  is a 3-weight cyclic code of length  $n = (r^2 - 1)/\delta$  and dimension  $3m$ . The weight distribution is given by Table 1.

Table 1: The weight distribution of  $\mathcal{C}_{(d_0, d_1)}^{(1)}$

Weight	Frequency
0	once
$\frac{q-1}{q\delta} (r^2 + r)$	$\frac{-1 + 3e - 2e^2 - q + 2eq + r^2 - 3er^2 + r^3 - 2er^3 + 2e^2r^3}{2e^2}$
$\frac{q-1}{q\delta} (r^2 - (e-1)r)$	$\frac{1 - 2e + r - er - r^2 + 2er^2 - r^3 + er^3}{e^2}$
$\frac{q-1}{q\delta} (r^2 - (2e-1)r)$	$\frac{-1 + e - r + r^2 - er^2 + r^3}{2e^2}$

From what follows we present some interesting examples of cyclic codes from  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  over GF(4) and GF(8) respectively which we find optimal or almost optimal by checking “Bounds on the minimum distance of linear codes” provided by the website <http://www.codetables.de/>. Note that these cyclic codes have only a few non-zero weights. Here we omit optimal cyclic codes which could be obtained from [16, 38] and hence only consider the case that  $(f, r - 1) > 1$ .

**Example 1.** Let  $q = 4, m = 2, r = 16, h = 1, f = 3$ . Then  $e = 1, (f, r - 1) = 3$ .

(1).  $t = 1$ :  $(d_0, d_1) = (51, 66)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(51, 66)}^{(1)}$  is a three-weight cyclic code with the weight enumerator

$$1 + 2040Y^{60} + 255Y^{64} + 1800Y^{68}.$$

This is a [85, 6, 60] code over GF(4) which is optimal among linear codes.

(2).  $t = 2$ :  $(d_0, d_1, d_2) = (51, 66, 81)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(51, 66, 81)}^{(1)}$  is a five-weight cyclic code with the weight enumerator

$$1 + 35700Y^{52} + 30600Y^{56} + 250920Y^{60} + 377655Y^{64} + 353700Y^{68}.$$

This is a [85, 10, 52] code over GF(4). It is known that for optimal linear codes of length 85 and dimension 10 over GF(4), the minimal distance satisfies  $52 \leq d \leq 56$ .

(3).  $t = 3$ :  $(d_0, d_1, d_2, d_3) = (51, 66, 81, 96)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(51,66,81,96)}^{(1)}$  is a seven-weight cyclic code with the weight enumerator  $1 + 185640Y^{44} + 464100Y^{48} + 4641000Y^{52} + 17646000Y^{56} + 54396600Y^{60} + 101483115Y^{64} + 89619000Y^{68}$ . This is a [85, 14, 44] code over GF(4). It is known that for optimal linear codes of length 85 and dimension 14 over GF(4), the minimal distance satisfies  $48 \leq d \leq 53$ .

**Example 2.** Let  $q = 8, m = 1, r = 8, h = 1, f = 7, r^2 = 64$ . Then  $e = 1, (f, r - 1) = 7$ .

(1).  $t = 1$ :  $(d_0, d_1) = (63, 70)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(63,70)}^{(1)}$  is a three-weight cyclic code with the weight enumerator

$$1 + 252Y^7 + 63Y^8 + 196Y^9.$$

This is a [9, 3, 7] code over GF(8) which is optimal among linear codes.

(2).  $t = 2$ :  $(d_0, d_1, d_2) = (63, 70, 77)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(63,70,77)}^{(1)}$  is a five-weight cyclic code with the weight enumerator

$$1 + 882Y^5 + 1764Y^6 + 7812Y^7 + 12411Y^8 + 9898Y^9.$$

This is a [9, 5, 5] code over GF(8) which is optimal among linear codes.

(3).  $t = 3$ :  $(d_0, d_1, d_2, d_3) = (63, 70, 77, 84)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(63,70,77,84)}^{(1)}$  is a seven-weight cyclic code with the weight enumerator

$$1 + 588Y^3 + 4410Y^4 + 33516Y^5 + 154056Y^6 + 463428Y^7 + 810621Y^8 + 630532Y^9.$$

This is a [9, 7, 3] code over GF(8) which is optimal among linear codes.

Now we present a table of cyclic codes from  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  over GF(3), GF(9), GF(5) and GF(7) respectively which we find optimal or almost optimal by checking “Bounds on the minimum distance of linear codes” provided by the website <http://www.codetables.de/>. For simplicity, only the parameters of the codes are listed. None of these cyclic codes can be obtained from [16, 38].

## 2.2 Cyclic code $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$

For any integers  $h, f$  and  $t \geq 1$ , define

$$e = (h, r + 1), \quad \delta = \begin{cases} \left(\frac{h+f}{2}(r-1) + f, r^2 - 1\right) & \text{if } t = 1 \\ \left(\frac{h+f}{2}(r-1) + f, (r-1)e\right) & \text{if } t \geq 2 \end{cases}, \quad n = (r^2 - 1)/\delta. \quad (6)$$

Assume that

$$(a'). \quad 1 \leq t \leq \frac{r+1}{2e},$$

$$(b'). \quad \text{if } p = 2, \text{ then } \left(f, \frac{r-1}{q-1}\right) = 1,$$

Table 2: Optimal or almost optimal cyclic codes from  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$

$q$	$r$	$(t =, h =, f =)$	code parameters	Optimal (?)
3	27	(1, 2, 1)	[182, 9, 108]	$111 \leq d \leq 115$ is optimal
9	9	(1, 1, 2)	[20, 3, 16]	$16 \leq d \leq 17$ is optimal
9	9	(1, 1, 4)	[10, 3, 8]	Y
9	9	(2, 1, 4)	[10, 5, 6]	Y
9	9	(3, 1, 4)	[10, 7, 4]	Y
9	9	(4, 1, 4)	[10, 9, 2]	Y
9	9	(1, 2, 8)	[5, 3, 3]	Y
5	5	(1, 1, 1)	[12, 3, 8]	Y
5	5	(1, 1, 2)	[6, 3, 4]	Y
5	5	(2, 1, 2)	[6, 5, 2]	Y
7	7	(1, 1, 2)	[24, 3, 18]	$d = 19$ is optimal
7	7	(1, 1, 3)	[8, 3, 6]	Y
7	7	(2, 1, 3)	[8, 5, 4]	Y
7	7	(3, 1, 3)	[8, 7, 2]	Y
7	7	(1, 2, 3)	[4, 3, 2]	Y

(c'). if  $p \geq 3$ , then

- (c1').  $h \equiv f \pmod{2}$  and  $\left(f, \frac{r-1}{q-1}\right) = 1$ , or
- (c2').  $h \equiv f \equiv 0 \pmod{2}$  and  $\left(\frac{f}{2}, \frac{r-1}{q-1}\right) = 1$ .

Let  $\tilde{d}_1, \dots, \tilde{d}_t$  be integers such that

$$\tilde{d}_j \equiv \left(j \cdot h + \frac{f-h}{2}\right) (r-1) + f \pmod{r^2-1}, \quad 1 \leq j \leq t. \quad (7)$$

Here if  $p = 2$ , the number  $\frac{1}{2}$  shall be interpreted as an integer which is the multiplicative inverse of 2  $\pmod{r-1}$ . It can be seen that  $(\tilde{d}_1, \dots, \tilde{d}_t, r^2-1) = \delta$ . The  $q$ -ary cyclic code  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  of length  $n$  consists of elements  $\tilde{c}(\underline{a})$  given by

$$\tilde{c}(\underline{a}) = \left( \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j \gamma^{\tilde{d}_j i} \right) \right)_{i=0}^{n-1}, \quad (8)$$

where  $\underline{a} = (a_1, \dots, a_t)$  for any  $a_1, \dots, a_t \in \text{GF}(r^2)$ . Note that the dual of  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  has the  $t$  zeroes  $\gamma^{-\tilde{d}_1}, \dots, \gamma^{-\tilde{d}_t}$ . Here  $\tilde{d}_j \equiv f \pmod{r-1} \forall j$ , the  $\gamma^{-\tilde{d}_j}$ 's are call the “generalized Niho type zeroes”.

We remark that a similar  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  over  $\text{GF}(p)$  was constructed in [38] under the condition  $(f, r-1) = 1$  (see [38, Theorem 1]). Clearly the conditions (b')(c') are more general and provide more flexible parameters. The weight distribution of  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  can be described as follows.

**Theorem 3.** (i). For  $p = 2$  or  $p$  being an odd prime, under assumptions (6)–(8) and (a')–(c'), the code  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  is a  $q$ -ary cyclic code of length  $n = (r^2 - 1)/\delta$  and dimension  $2tm$ , with at most  $2t$  non-zero weights, each of which is given by

$$\tilde{w}_j = \frac{q-1}{q\delta} \cdot (r^2 - (je - 1)r), \quad 0 \leq j \leq 2t - 1.$$

(ii). Let  $\tilde{\mu}_j$  be the frequency of the weight  $\tilde{w}_j$  for each  $j$ . Define  $\tilde{\underline{\mu}} = (\tilde{\mu}_0, \tilde{\mu}_1, \dots, \tilde{\mu}_{2t-1})^T$ , and  $\tilde{\underline{b}} = (\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{2t-1})^T$  where  $\tilde{b}_i = r^{2t}N_i - (r^2 - 1)^i$ . Then

$$\tilde{\underline{\mu}} = \left( M_t^{(2)} \right)^{-1} \tilde{\underline{b}}.$$

Here  $M_t^{(2)} = [m_{ij}]_{0 \leq i,j \leq 2t-1}$  is a  $2t \times 2t$  Vandermonde matrix whose entry is given by  $m_{ij} := (jer - r - 1)^i$ .

**Corollary 4.** (i). Under assumptions (6)–(8) and (a')–(c') for  $t = 1$ , the code  $\mathcal{C}_{(\tilde{d}_1)}^{(2)}$  is a  $q$ -ary cyclic code of length  $n = (r^2 - 1)/\delta$  and dimension  $2m$  with most two non-zero weights. The weight distribution is given by Table 3. Note that it is a 1-weight code if and only if  $e = 1$ .

(ii). Under assumptions (6)–(8) and (a')–(c') for  $t = 2$ , the code  $\mathcal{C}_{(\tilde{d}_1, \tilde{d}_2)}^{(2)}$  is a 4-weight cyclic code of length  $n = (r^2 - 1)/\delta$  and dimension  $4m$ . The weight distribution is given by Table 4.

Since  $\mathcal{C}_{(\tilde{d}_1)}^{(2)}$  is irreducible, (i) of Corollary 4 should be known to researchers in the field. We collect the result here only for the sake of completeness. However, the dual of  $\mathcal{C}_{(\tilde{d}_1, \tilde{d}_2)}^{(2)}$  has two zeroes, and (ii) of Corollary 4 is new.

Table 3: The weight distribution of  $\mathcal{C}_{(\tilde{d}_1)}^{(2)}$

Weight	Frequency
0	once
$\frac{q-1}{q\delta} (r^2 + r)$	$\frac{(e-1)(r^2-1)}{e}$
$\frac{q-1}{q\delta} (r^2 - (e-1)r)$	$\frac{r^2-1}{e}$

From what follows we present some interesting examples of cyclic codes from  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  over GF(4) and GF(8) respectively which we find optimal or almost optimal by checking “Bounds on the minimum distance of linear codes” provided by the website <http://www.codetables.de/>. Note that these cyclic codes have only a few non-zero weights. Here we omit optimal cyclic codes which could be obtained from [16, 38] and hence only consider the case that  $(f, r - 1) > 1$ .

**Example 3.** Let  $q = 4, m = 2, r = 16, h = 2, f = 6$ . Then  $e = 1, (f, r - 1) = 3$ .

- (1).  $t = 1$ :  $(\tilde{d}_1) = (66)$ . Both Theorem 3 and numerical computation by **Magma** show that  $\mathcal{C}_{(66)}^{(1)}$  is a one-weight cyclic code with the weight enumerator

$$1 + 255Y^{64}.$$

This is a [85, 4, 64] code over GF(4) which is optimal among linear codes.

Table 4: The weight distribution of  $\mathcal{C}_{(\tilde{d}_1, \tilde{d}_2)}^{(2)}$

Weight	Frequency
0	once
$\frac{q-1}{q\delta} (r^2 + r)$	$\frac{1-6e+11e^2-6e^3+2r-9er+9e^2r+3er^2-5e^2r^2-2r^3+9er^3-9e^2r^3-r^4+3er^4-6e^2r^4+6e^3r^4}{6e^3}$
$\frac{q-1}{q\delta} (r^2 - (e-1)r)$	$\frac{-1+5e-6e^2-2r+7er-4e^2r-3er^2+4e^2r^2+2r^3-7er^3+4e^2r^3+r^4-2er^4+2e^2r^4}{2e^3}$
$\frac{q-1}{q\delta} (r^2 - (2e-1)r)$	$\frac{1-4e+3e^2+2r-5er+e^2r+3er^2-3e^2r^2-2r^3+5er^3-e^2r^3-r^4+er^4}{2e^3}$
$\frac{q-1}{q\delta} (r^2 - (3e-1)r)$	$\frac{-1+3e-2e^2-2r+3er-3er^2+2e^2r^2+2r^3-3er^3+r^4}{6e^3}$

(2).  $t = 2$ :  $(\tilde{d}_1, \tilde{d}_2) = (66, 96)$ . Both Theorem 3 and numerical computation by **Magma** show that  $\mathcal{C}_{(66, 96)}^{(1)}$  is a four-weight cyclic code with the weight enumerator

$$1 + 10200Y^{56} + 4080Y^{60} + 30855Y^{64} + 20400Y^{68}.$$

This is a [85, 8, 56] code over GF(4). It is known that for optimal linear codes of length 85 and dimension 8 over GF(4), the minimal distance satisfies  $56 \leq d \leq 59$ .

(3).  $t = 3$ :  $(\tilde{d}_1, \tilde{d}_2, \tilde{d}_3) = (66, 96, 126)$ . Both Theorem 3 and numerical computation by **Magma** show that  $\mathcal{C}_{(66, 96, 126)}^{(1)}$  is a six-weight cyclic code with the weight enumerator  $1 + 92820Y^{48} + 142800Y^{52} + 1285200Y^{56} + 3272160Y^{60} + 6390555Y^{64} + 5593680Y^{68}$ . This is a [85, 12, 48] code over GF(4). It is known that for optimal linear codes of length 85 and dimension 12 over GF(4), the minimal distance satisfies  $48 \leq d \leq 55$ .

**Example 4.** Let  $q = 8, m = 1, r = 8, h = 2, f = 14, r^2 = 64$ . Then  $e = 1, (f, r-1) = 7$ .

(1).  $t = 1$ :  $(\tilde{d}_1) = (70)$ . Both Theorem 1 and numerical computation by **Magma** show that  $\mathcal{C}_{(70)}^{(2)}$  is a one-weight cyclic code with the weight enumerator

$$1 + 63Y^8.$$

This is a [9, 2, 8] code over GF(8) which is optimal among linear codes.

(2).  $t = 2$ :  $(\tilde{d}_1, \tilde{d}_2) = (70, 84)$ . Both Theorem 3 and numerical computation by **Magma** show that  $\mathcal{C}_{(70, 84)}^{(2)}$  is a four-weight cyclic code with the weight enumerator

$$1 + 588Y^6 + 504Y^7 + 1827Y^8 + 1176Y^9.$$

This is a [9, 4, 6] code over GF(8) which is optimal among linear codes.

(3).  $t = 3$ :  $(\tilde{d}_1, \tilde{d}_2, \tilde{d}_3) = (70, 84, 98)$ . Both Theorem 3 and numerical computation by **Magma** show that  $\mathcal{C}_{(70, 84, 98)}^{(2)}$  is a six-weight cyclic code with the weight enumerator

$$1 + 882Y^4 + 3528Y^5 + 19992Y^6 + 57456Y^7 + 101493Y^8 + 78792Y^9.$$

This is a [9, 6, 4] code over GF(8) which is optimal among linear codes.

Now we present a table of cyclic codes from  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  over GF(3), GF(9), GF(5) and GF(7) respectively which we find optimal or almost optimal by checking “Bounds on the minimum distance of linear codes” from the website <http://www.codetables.de/>. For simplicity, only the parameters of the code are listed. Note that none of these cyclic codes can be obtained from [16, 38].

Table 5: Optimal or almost optimal cyclic codes from  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$

$q$	$r$	$(t =, h =, f =)$	code parameters	Optimal (?)
3	27	(1, 4, 2)	[91, 6, 54]	$57 \leq d \leq 58$ is optimal
9	9	(1, 2, 8)	[5, 2, 4]	Y
9	9	(2, 2, 8)	[5, 4, 2]	Y
7	7	(1, 1, 3)	[16, 2, 14]	Y
7	7	(2, 1, 3)	[16, 4, 10]	$d = 11$ is optimal

### 3 Preliminaries

Following notation from Section 2, let  $p$  be a prime,  $q = p^l, r = q^m$  and let  $\gamma$  be a primitive element of  $\text{GF}(r^2)$ . Define  $\text{GF}(r^2)^* := \text{GF}(r^2) - \{0\}$ . For any integer  $d$ , let  $h_d(x) \in \text{GF}(q)[x]$  be the minimal polynomial of  $\gamma^{-d}$  over  $\text{GF}(q)$ . We first prove the following lemma, the proof of which is similar to [38, Lemma 5].

**Lemma 5.** Suppose  $\left(\Delta, \frac{r-1}{q-1}\right) = 1$  or  $\left(\frac{\Delta}{2}, \frac{r-1}{q-1}\right) = 1$  if  $\Delta$  is even.

(i). If  $d = s(r-1) + \Delta$ , then  $\deg h_d(x) = \begin{cases} m & : \text{if } \Delta \equiv 2s \pmod{r+1}, \\ 2m & : \text{if } \Delta \not\equiv 2s \pmod{r+1}. \end{cases}$

(ii). If  $d = s(r-1) + \Delta$  and  $d' = s'(r-1) + \Delta$ , then  $h_d(x) = h_{d'}(x)$  if and only if  $s \equiv s' \pmod{r+1}$  or  $s + s' \equiv \Delta \pmod{r+1}$ .

*Proof.* (i).  $\deg h_d(x)$  is the least positive integer  $k$ ,  $1 \leq k \leq 2m$  such that  $dq^k \equiv d \pmod{r^2 - 1}$ . Since  $d \equiv \Delta \pmod{r-1}$ , we have  $(q^m - 1)|\Delta(q^k - 1)$ . Dividing  $q-1$  on both sides, we find that  $(q^m - 1)|2(q^k - 1)$ . Let  $\nu = (m, k)$  and  $\lambda = \frac{q^m - 1}{q^\nu - 1}$ . Then  $\left(\lambda, \frac{q^k - 1}{q^\nu - 1}\right) = 1$ , and we have  $\lambda|2$ . If  $\lambda = 2$ , then  $m \geq 2$  and  $\nu < m$ , hence  $\nu \leq \frac{m}{2}$ . We have  $q^m - 1 = 2(q^\nu - 1) \leq 2(q^{m/2} - 1)$ . This implies that  $q \leq q^{m/2} < 2$ , contradiction. So we must have  $\lambda = \frac{q^m - 1}{q^\nu - 1} = 1$ , that is,  $\nu = m$ , hence  $k = m$  or  $2m$ .

If  $k = m$ , this is equivalent to  $d(r-1) \equiv 0 \pmod{r^2 - 1}$ , that is  $d \equiv 0 \pmod{r+1}$ , and hence  $(r+1)|(\Delta - 2s)$ . If  $(r+1) \nmid (\Delta - 2s)$ , we must have  $k = 2m$ .

(ii).  $h_d(x) = h_{d'}(x)$  if and only if there exists an integer  $k$ ,  $1 \leq k \leq 2m$  such that  $dq^k \equiv d' \pmod{r^2 - 1}$ . Reducing the equation modulo  $r-1$ , by similar argument we find that  $k = m$  or  $2m$ . If  $k = 2m$ , then obviously  $s \equiv s' \pmod{r+1}$ . Otherwise  $k = m$ , we have  $(s(r-1) + \Delta)r \equiv s'(r-1) + \Delta \pmod{r^2 - 1}$ . This is equivalent to  $\Delta \equiv s + s' \pmod{r+1}$  by simple computation. This completes the proof of Lemma 5.  $\square$

From Lemma 5 we immediately obtain the following.

**Lemma 6.** (1). For  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$ , let assumptions be as in Theorem 1. Then

(i).  $\deg h_{d_0}(x) = m$  and  $\deg h_{d_i}(x) = 2m, \forall 1 \leq i \leq t$ .

(ii).  $h_{d_i}(x) \neq h_{d_j}(x)$  for any  $0 \leq i \neq j \leq t$ .

(2). For  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$ , let assumptions be as in Theorem 3. Then

(i).  $\deg h_{\tilde{d}_i}(x) = 2m, \forall 1 \leq i \leq t$ .

(ii).  $h_{\tilde{d}_i}(x) \neq h_{\tilde{d}_j}(x)$  for any  $1 \leq i \neq j \leq t$ .

## 4 $p = 2$ : Proofs of (i) of Theorems 1 and 3

We first prove Statement (i) of Theorem 1. By Delsarte's Theorem [5] and Lemma 6,  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  is a cyclic code of length  $n$  with parity-check polynomial given by  $\prod_{i=0}^t h_{d_i}(x)$ , which is of degree  $(2t+1)m$ , hence  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  has dimension  $(2t+1)m$  over  $\text{GF}(q)$ . Since

$$\delta = (d_0, \dots, d_t, r^2 - 1) = ((r+1)f, (r-1)e),$$

we see that the Hamming weight of a codeword  $c(\underline{a})$  can be expressed as

$$\begin{aligned} \delta \omega_H(c(\underline{a})) &= r^2 - \# \left\{ x \in \text{GF}(r^2) : \text{Tr}_{r/q}(a_0 x^{d_0}) + \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j x^{d_j} \right) = 0 \right\} \\ &= r^2 - \frac{1}{q} \sum_{x \in \text{GF}(r^2)} \sum_{\lambda \in \text{GF}(q)} \psi_q \left\{ \lambda \text{Tr}_{r/q}(a_0 x^{d_0}) + \lambda \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j x^{d_j} \right) \right\} \\ &= r^2 \left( 1 - \frac{1}{q} \right) - \frac{S(\underline{a})}{q}, \end{aligned}$$

where  $\psi_q : \text{GF}(q) \rightarrow \mathbb{C}^*$  is the standard additive character given by  $\psi_q(x) = \zeta_p^{\text{Tr}_{q/p}(x)}$  for any  $x \in \text{GF}(q)$ ,  $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ , and

$$S(\underline{a}) := (q-1) + \sum_{\lambda \in \text{GF}(q)^*} \sum_{x \in \text{GF}(r^2)^*} \psi_q \left\{ \lambda \text{Tr}_{r/q}(a_0 x^{d_0}) + \lambda \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j x^{d_j} \right) \right\}. \quad (9)$$

Since  $(r-1, r+1) = 1$ , we can write each  $x \in \text{GF}(r^2)^*$  uniquely as  $x = yz$  for  $y \in \text{GF}(r)^*$  and  $z \in U := \{\omega \in \text{GF}(r^2) : \bar{\omega}\omega = \omega^{r+1} = 1\}$ . Here we denote  $\bar{x} := x^r$ . Note that  $U$  is a cyclic subgroup of  $\text{GF}(r^2)^*$  generated by  $\gamma^{r-1}$ . Since  $y^r = y$  for any  $y \in \text{GF}(r)$ , from (2) we have

$$x^{d_j} = y^{d_j} z^{d_j} = y^{2f} z^{-2jh}, \forall j,$$

and

$$x^{rd_j} = y^{2rf} z^{-2rjh} = y^{2f} z^{2jh}, \forall j.$$

Hence

$$S(\underline{a}) = (q-1) + \sum_{z \in U} \sum_{y \in \text{GF}(r)^*} \sum_{\lambda \in \text{GF}(q)^*} \psi_r \left\{ \lambda y^{2f} \left( a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} \right) \right\}.$$

Here  $\psi_r : \text{GF}(r) \rightarrow \{\pm 1\}$  is the standard additive character. Since  $\left(2f, \frac{r-1}{q-1}\right) = \left(f, \frac{r-1}{q-1}\right) = 1$ , we observe that as  $\lambda$  runs over  $\text{GF}(q)^*$  and  $y$  runs over  $\text{GF}(r)^*$  respectively, the value  $\lambda y^{2f}$  will run over each element of  $\text{GF}(r)^*$  exactly  $(q-1)$  times. Hence we obtain

$$S(\underline{a}) = (q-1) + (q-1) \sum_{z \in U} \sum_{y \in \text{GF}(r)^*} \psi_r \left\{ y \left( a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} \right) \right\}.$$

Clearly  $S(\underline{a}) = (q-1)r(N-1)$ , where  $N$  is the number of  $z \in U$  such that

$$a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} = 0.$$

Letting  $u = z^{-2h}$  and multiplying  $u^t$  on both sides, we find

$$a_0 u^t + \sum_{j=1}^t a_j u^{t+j} + \bar{a}_j u^{t-j} = 0.$$

This is a polynomial of degree at most  $2t$ , it may have  $0, 1, \dots$ , or  $2t$  solutions for  $u$ , and for each such  $u \in U$ , the number of  $z \in U$  such that  $z^{-2h} = u$  is always  $e = (2h, r+1) = (h, r+1)$ . Hence the possible values of  $N$  are  $je, \forall 0 \leq j \leq 2t$ . This indicates that  $S(\underline{a})$  and  $\omega_H(c(\underline{a}))$  take at most  $(2t+1)$  distinct values. This proves (i) of Theorem 1.

Statement (i) of Theorem 3 can be proved similarly by using the above idea and by modifying the proof of [38, Theorem 1] for  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  accordingly. We omit the details.  $\square$

## 5 $p = 2$ : Proofs of (ii) of Theorems 1 and 3

Since it is proved that there are only a few non-zero weights in  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  and  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$ , a standard procedure to determine the weight distribution is to compute power moment identities.

We now prove Statement (ii) of Theorem 1. Let  $\mu_j$  be the frequency of weight  $w_j$  for each  $j$ . Obviously  $S(\underline{a}) = (q-1)r^2$  if and only if  $\underline{a} = \underline{0}$ . We have

$$r^{1+2t} = 1 + \sum_{j=0}^{2t} \mu_j, \tag{10}$$

and for any positive integer  $k$ ,

$$\sum_{\substack{a_0 \in \text{GF}(r) \\ a_j \in \text{GF}(r^2), 1 \leq j \leq t}} (S(\underline{a}) - (q-1))^k = (q-1)^k (r^2 - 1)^k + \sum_{j=0}^{2t} (q-1)^k (jer - r - 1)^k \mu_j. \tag{11}$$

On the other hand, by the orthogonal relation

$$\frac{1}{r^2} \sum_{x \in \text{GF}(r^2)} \psi_q \left\{ \text{Tr}_{r^2/q}(xa) \right\} = \begin{cases} 0 & : \text{ if } a \in \text{GF}(r^2)^* \\ 1 & : \text{ if } a = 0, \end{cases}$$

we find easily that

$$\sum_{\substack{a_0 \in \text{GF}(r) \\ a_j \in \text{GF}(r^2), 1 \leq j \leq t}} (S(\underline{a}) - 1)^k = r^{1+2t} M_k, \quad (12)$$

where  $M_k$  denotes the number of solutions  $(\lambda_1, \dots, \lambda_k) \in (\text{GF}(q)^*)^k$  and  $(x_1, \dots, x_k) \in (\text{GF}(r^2)^*)^k$  that satisfy the equations

$$\begin{cases} \lambda_1 x_1^{d_0} + \lambda_2 x_2^{d_0} + \dots + \lambda_k x_k^{d_0} = 0, \\ \lambda_1 x_1^{d_1} + \lambda_2 x_2^{d_1} + \dots + \lambda_k x_k^{d_1} = 0, \\ \dots \\ \lambda_1 x_1^{d_t} + \lambda_2 x_2^{d_t} + \dots + \lambda_k x_k^{d_t} = 0. \end{cases} \quad (13)$$

Lemma 7 which we will prove below states that  $M_k = (q-1)^k N_k$  for any  $1 \leq k \leq 2t$ , where  $N_k$  is given by the formula (4). Combining this with identities (10), (11) and (12) for  $1 \leq k \leq 2t$ , we obtain the matrix equation

$$M_t^{(1)} \cdot \underline{\mu} = \underline{b},$$

where  $M_t^{(1)}$ ,  $\underline{\mu}$  and  $\underline{b}$  are explicitly defined in Theorem 1. Since  $M_t^{(1)}$  is invertible, we obtain  $\underline{\mu} = (M_t^{(1)})^{-1} \cdot \underline{b}$ , as claimed by (ii) of Theorem 1. Now we prove the technical lemma.

**Lemma 7.**  $M_k = (q-1)^k N_k$  for any  $1 \leq k \leq 2t$ , where  $N_k$  is given by the formula (4).

*Proof.* Using the same notation as before, we may write each  $x_i \in \text{GF}(r^2)^*$  as

$$x_i = y_i z_i, \quad y_i \in \text{GF}(r)^*, z_i \in U. \quad (14)$$

Since

$$x_i^{d_j} = y_i^{2f} z_i^{-2jh}, \quad \forall i, j,$$

The equations (13) can be written as

$$\sum_{i=1}^k \lambda_i \cdot y_i^{2f} z_i^{-2jh} = 0, \quad \forall 0 \leq j \leq t. \quad (15)$$

Since  $\left(2f, \frac{r-1}{q-1}\right) = 1$ ,  $\lambda_i \cdot y_i^{2f}$  takes each value of  $\text{GF}(r)^*$  exactly  $(q-1)$  times as  $\lambda_i$  and  $y_i$  run over the sets  $\text{GF}(q)^*$  and  $\text{GF}(r)^*$  respectively. So  $M_k = (q-1)^k M_{k,1}$  where  $M_{k,1}$  counts the number of  $y_i \in \text{GF}(r)^*$ ,  $z_i \in U \forall i$  such that

$$\sum_{i=1}^k y_i z_i^{-2jh} = 0, \quad \forall 0 \leq j \leq t. \quad (16)$$

In [38] we have used a combinatorial method to obtain the number of solutions to equations (16). Roughly speaking, let  $u_i = z_i^{-2h} \in U^e$  where  $e = (2h, r+1) = (h, r+1)$ . Using  $y_i, u_i$ 's, we can write (16) as a matrix equation  $\mathbf{A} \cdot \underline{y} = \underline{0}$  where

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2 & \cdots & u_k \\ u_1^2 & u_2^2 & \cdots & u_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ u_1^t & u_2^t & \cdots & u_k^t \end{bmatrix}, \quad \underline{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix}.$$

We observe that  $\mathbf{A}$  is a Vandermonde matrix. We may take the  $r$ -th power of each equation to obtain additional  $(t-1)$  equations. It turns out that for any  $1 \leq k \leq 2t$  there are only “trivial” solutions which can be counted exactly by using combinatorial argument. We conclude that  $M_{k,1} = N_k$ , which is given by the formula (4). Interested readers may review [38] for details. Therefore we obtain  $M_k = (p-1)^k N_k$  as desired.

Statement (ii) of Theorem 3 can be proved similarly, by using the above idea and by modifying the proof of [38, Theorem 2] for  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  accordingly. We omit the details.  $\square$

## 6 $p \geq 3$ : Proofs of (i) of Theorems 1 and 3

We first prove Statement (i) of Theorem 1. Similar to the case that  $p = 2$ ,  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  is a cyclic code of length  $n$  with parity-check polynomial given by  $\prod_{i=0}^t h_{d_i}(x)$ , which is of degree  $(2t+1)m$ , hence  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}$  has dimension  $(2t+1)m$  over  $\text{GF}(q)$ , and the Hamming weight of a codeword  $c(\underline{a})$  can be expressed as

$$\delta\omega_H(c(\underline{a})) = r^2 \left(1 - \frac{1}{q}\right) - \frac{S(\underline{a})}{q},$$

where

$$S(\underline{a}) := (q-1) + \sum_{\lambda \in \text{GF}(q)^*} \sum_{x \in \text{GF}(r^2)^*} \psi_q \left\{ \lambda \text{Tr}_{r/q} (a_0 x^{d_0}) + \lambda \text{Tr}_{r^2/q} \left( \sum_{j=1}^t a_j x^{d_j} \right) \right\}. \quad (17)$$

### 6.1 Case 1: $m$ is odd.

We write each  $x \in \text{GF}(r^2)^*$  uniquely as  $x = yw$  for  $y \in \text{GF}(r)^*$  and  $w \in \Omega = \{1, \gamma, \gamma^2, \dots, \gamma^r\}$  (see also [16, Lemma 2]). We may observe that  $U := \{\alpha^{r-1} : \alpha \in \Omega\}$  is a cyclic subgroup of  $\text{GF}(r^2)^*$  generated by  $\gamma^{r-1}$ . Since  $y^r = y$  for any  $y \in \text{GF}(r)$ , from (2) we have

$$x^{d_j} = y^{d_j} \omega^{d_j} = y^{2f} \omega^{d_j}, \forall j,$$

and

$$x^{rd_j} = y^{2fr} \omega^{rd_j} = y^{2f} \bar{\omega}^{d_j}, \forall j.$$

Here we denote  $\bar{x} := x^r$ . Hence

$$S(\underline{a}) = (q-1) + \sum_{w \in \Omega} \sum_{y \in \text{GF}(r)^*} \sum_{\lambda \in \text{GF}(q)^*} \psi_q \left\{ \text{Tr}_{r/q} \left( \lambda y^{2f} \left\{ a_0 \omega^{d_0} + \sum_{j=1}^t a_j \omega^{d_j} + \bar{a}_j \bar{\omega}^{d_j} \right\} \right) \right\}.$$

Since  $\frac{r-1}{q-1} \equiv m \pmod{2}$  is odd,  $\left(2f, \frac{r-1}{q-1}\right) = \left(f, \frac{r-1}{q-1}\right) = 1$ . We observe that as  $\lambda$  runs over  $\text{GF}(q)^*$  and  $y$  runs over  $\text{GF}(r)^*$  respectively, the value  $\lambda y^{2f}$  will run over each element of  $\text{GF}(r)^*$  exactly  $(q-1)$  times. Hence we obtain

$$S(\underline{a}) = (q-1) + (q-1) \sum_{\omega \in \Omega} \sum_{y \in \text{GF}(r)^*} \psi_q \left\{ \text{Tr}_{r/q} \left( y \left\{ a_0 \omega^{d_0} + \sum_{j=1}^t a_j \omega^{d_j} + \bar{a}_j \bar{\omega}^{d_j} \right\} \right) \right\}.$$

Clearly  $S(\underline{a}) = (q-1)r(N-1)$ , where  $N$  is the number of  $\omega \in \Omega$  such that

$$a_0 \omega^{d_0} + \sum_{j=1}^t a_j \omega^{d_j} + \bar{a}_j \omega^{rd_j} = 0.$$

Dividing  $\omega^{d_0}$  on both sides and writing  $z = \omega^{r-1} \in U$ , the equation becomes

$$a_0 + \sum_{j=1}^t a_j z^{jh} + \bar{a}_j z^{-jh} = 0.$$

Letting  $u = z^h$  and multiplying  $u^t$  on both sides, we find

$$a_0 u^t + \sum_{j=1}^t a_j u^{t+j} + \bar{a}_j u^{t-j} = 0.$$

This is a polynomial of degree at most  $2t$ , so possibly it may have  $0, 1, \dots$ , or  $2t$  solutions for  $u$ , and for each such  $u \in U$ , the number of  $z \in U$  such that  $z^h = u$  is always  $e = (h, r+1)$ . Hence the possible values of  $N$  are  $je, \forall 0 \leq j \leq 2t$ . This indicates that  $S(\underline{a})$  and  $\omega_H(c(\underline{a}))$  take at most  $(2t+1)$  distinct values. This proves (i) of Theorem 1 when  $m$  is odd.

## 6.2 Case 2: $m$ and $h$ are both even.

For this case we use a different strategy. Since

$$\text{GF}(r)^* \cap U = \{-1, 1\},$$

we may write each  $x \in \text{GF}(r^2)^*$  as

$$x = yz\epsilon, \quad x \in \text{GF}(r)^*, z \in U, \epsilon \in \{\xi, 1\}, \quad (18)$$

where  $\xi \in \text{GF}(r^2)^*$  is a fixed non-square,  $U$  is the cyclic subgroup of  $\text{GF}(r^2)^*$  generated by  $\gamma^{r-1}$ . We may choose  $\xi = \gamma^{(r+1)/2}$  as  $r = q^m \equiv 1 \pmod{4}$ . It is clear that as  $y, z, \epsilon$  run over the sets  $\text{GF}(r)^*, U$  and  $\{\xi, 1\}$  respectively, the value  $x$  will run over each element of  $\text{GF}(r^2)^*$  exactly twice. Also observing

$$x^{d_j} = (yz\epsilon)^{d_j} = (y^2 \epsilon^{r+1})^f z^{-2jh} \epsilon^{(r-1)jh}, \forall j,$$

$$x^{rd_j} = (yz\epsilon)^{rd_j} = (y^2 \epsilon^{r+1})^f z^{2jh} \epsilon^{-(r-1)jh}, \forall j,$$

and

$$\xi^{(r-1)h} = (\gamma^{(r^2-1)})^{h/2} = 1,$$

we can rewrite (17) as

$$S(\underline{a}) = (q-1) + \frac{1}{2} \sum_{\lambda \in \text{GF}(q)^*} \sum_{\substack{y \in \text{GF}(r)^* \\ z \in U \\ \epsilon \in \{\xi, 1\}}} \psi_q \left\{ \text{Tr}_{r/q} \left( \lambda (y^2 \epsilon^{r+1})^f \left\{ a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} \right\} \right) \right\}.$$

Next we observe that  $\xi^{r+1} = (\gamma^{r+1})^{(r+1)/2}$  is a non-square in  $\text{GF}(r)^*$ , so as  $y$  runs over  $\text{GF}(r)^*$  and  $\epsilon$  runs over  $\{\xi, 1\}$  respectively, the value  $y^2 \epsilon^{r+1}$  will run over each element of  $\text{GF}(r)^*$  exactly twice. Therefore we obtain

$$S(\underline{a}) = (q-1) + \sum_{z \in U} \sum_{\lambda \in \text{GF}(q)^*} \sum_{y \in \text{GF}(r)^*} \psi_q \left\{ \text{Tr}_{r/q} \left( \lambda y^f \left\{ a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} \right\} \right) \right\}.$$

Since  $\left(f, \frac{r-1}{q-1}\right) = 1$ ,  $\lambda y^f$  will take each value of  $\text{GF}(r)^*$  exactly  $(q-1)$  times as  $y, \lambda$  runs over  $\text{GF}(r)^*$  and  $\text{GF}(q)^*$  respectively. So

$$\begin{aligned} S(\underline{a}) &= (q-1) + (q-1) \sum_{z \in U} \sum_{y \in \text{GF}(r)^*} \psi_q \left\{ \text{Tr}_{r/q} \left( y \left\{ a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} \right\} \right) \right\} \\ &= (q-1)r(N-1), \end{aligned}$$

where  $N$  is the number of  $z \in U$  such that

$$a_0 + \sum_{j=1}^t a_j z^{-2jh} + \bar{a}_j z^{2jh} = 0.$$

Letting  $u = z^{-2h}$  and multiplying  $u^t$  on both sides, we find

$$a_0 u^t + \sum_{j=1}^t a_j u^{t+j} + \bar{a}_j u^{t-j} = 0.$$

This yields at most  $2t$  solutions for  $u$ , and for each such  $u$ , the number of  $z \in U$  such that  $z^{-2h} = u$  is exactly  $(-2h, r+1) = (h, r+1) = e$  because  $r \equiv 1 \pmod{4}$  and  $2|h$ . Hence  $N \in \{je : 0 \leq j \leq 2t\}$ . This indicates again that  $S(\underline{a})$  and  $\omega_H(c(\underline{a}))$  take at most  $(2t+1)$  distinct values. This concludes the case for both  $m$  and  $h$  being even. Now (i) of Theorem 1 is proved.

Statement (i) of Theorem 3 can be proved similarly by using the above idea and by modifying the proof of [38, Theorem 1] for  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  accordingly. We omit the details.  $\square$

## 7 $p \geq 3$ : Proofs of (ii) of Theorems 1 and 3

We now prove Statement (ii) of Theorem 1. Let  $\mu_j$  be the frequency of weight  $w_j$  for each  $j$ . Similar to the case  $p = 2$ , we have

$$r^{1+2t} = 1 + \sum_{j=0}^{2t} \mu_j, \tag{19}$$

and for any positive integer  $k$ ,

$$\sum_{\substack{a_0 \in \text{GF}(r) \\ a_j \in \text{GF}(r^2), 1 \leq j \leq t}} (S(\underline{a}) - (q-1))^k = (q-1)^k (r^2-1)^k + \sum_{j=0}^{2t} (q-1)^k (jer - r - 1)^k \mu_j, \quad (20)$$

and

$$\sum_{\substack{a_0 \in \text{GF}(r) \\ a_j \in \text{GF}(r^2), 1 \leq j \leq t}} (S(\underline{a}) - 1)^k = q^{1+2t} M_k, \quad (21)$$

where  $M_k$  denotes the number of solutions  $(\lambda_1, \dots, \lambda_k) \in (\text{GF}(q)^*)^k$  and  $(x_1, \dots, x_k) \in (\text{GF}(r^2)^*)^k$  that satisfy the equations

$$\begin{cases} \lambda_1 x_1^{d_0} + \lambda_2 x_2^{d_0} + \cdots + \lambda_k x_k^{d_0} = 0, \\ \lambda_1 x_1^{d_1} + \lambda_2 x_2^{d_1} + \cdots + \lambda_k x_k^{d_1} = 0, \\ \cdots \\ \lambda_1 x_1^{d_t} + \lambda_2 x_2^{d_t} + \cdots + \lambda_k x_k^{d_t} = 0. \end{cases} \quad (22)$$

Lemma 8 which we will prove below states that that  $M_k = (q-1)^k N_k$  for any  $1 \leq k \leq 2t$ , where  $N_k$  is given by the formula (4). Combining this with identities (19), (20) and (21) for  $1 \leq k \leq 2t$ , we obtain the matrix equation

$$M_t^{(1)} \cdot \underline{\mu} = \underline{b},$$

where  $M_t^{(1)}$ ,  $\underline{\mu}$  and  $\underline{b}$  are explicitly defined in Theorem 1. Since  $M_t^{(1)}$  is invertible, we obtain  $\underline{\mu} = (M_t^{(1)})^{-1} \cdot \underline{b}$ , as claimed by (ii) of Theorem 1. Now we prove the technical lemma.

**Lemma 8.**  $M_k = (q-1)^k N_k$  for any  $1 \leq k \leq 2t$ , where  $N_k$  is given by the formula (4).

*Proof.* Using the same notation as before, we may write each  $x_i \in \text{GF}(r^2)^*$  as

$$x_i = y_i z_i \epsilon_i, \quad y_i \in \text{GF}(r)^*, z_i \in U, \epsilon_i \in \{\xi, 1\}, \quad (23)$$

where  $\xi \in \text{GF}(r^2)^*$  is a fixed non-square. As  $y_i, z_i, \epsilon_i$  run over the sets  $\text{GF}(r)^*$ ,  $U$  and  $\{\xi, 1\}$  respectively,  $x_i = y_i z_i \epsilon_i$  will run over each element of  $\text{GF}(r^2)^*$  exactly twice. So  $M_k = 2^{-k} M_{k,1}$  where  $M_{k,1}$  is the number of  $\lambda_i \in \text{GF}(q)^*$ ,  $y_i \in \text{GF}(r)^*$ ,  $z_i \in U$ ,  $\epsilon_i \in \{\xi, 1\}$ ,  $1 \leq i \leq r$  such that  $\lambda_i, x_i = y_i z_i \epsilon_i \forall i$  satisfy the equations (22) simultaneously. Since

$$x_i^{d_j} = (y_i^2 \epsilon_i^{r+1})^f (z_i^{-2} \epsilon_i^{r-1})^{jh}, \quad \forall j,$$

The equations (22) can be written as

$$\sum_{i=1}^k \lambda_i \cdot (y_i^2 \epsilon_i^{r+1})^f (z_i^{-2} \epsilon_i^{r-1})^{jh} = 0, \quad \forall 0 \leq j \leq t. \quad (24)$$

## 7.1 Case 1: $m$ is odd

Then  $\frac{r-1}{q-1} \equiv m \equiv 1 \pmod{2}$ , we may take  $\xi = \gamma^{(r-1)/(q-1)}$ . Then  $\xi^{r+1} = \gamma^{(r^2-1)/(q-1)} \in \text{GF}(q)^*$ . For each fixed  $\epsilon_i$ , denoting  $\lambda'_i = \lambda_i \epsilon_i^{(r+1)f} \in \text{GF}(q)^*$ , so to find  $M_{k,1}$ , it is equivalent to count the number of  $\lambda'_i \in \text{GF}(q)^*, y_i \in \text{GF}(r)^*, z_i \in U, \epsilon_i \in \{\xi, 1\} \forall i$  such that

$$\sum_{i=1}^k \lambda'_i \cdot y_i^{2f} (z_i^{-2} \epsilon_i^{r-1})^{jh} = 0, \forall 0 \leq j \leq t.$$

Since  $\left(2f, \frac{r-1}{q-1}\right) = 1$ ,  $\lambda'_i \cdot y_i^{2f}$  takes each value of  $\text{GF}(r)^*$  exactly  $(q-1)$  times as  $\lambda'_i$  and  $y_i$  run over the sets  $\text{GF}(q)^*$  and  $\text{GF}(r)^*$  respectively. Moreover,  $\xi^{r-1} = (\gamma^{r-1})^{(r-1)/(q-1)}$  is a non-square in  $U$ , hence  $z_i^{-2} \epsilon_i^{r-1}$  takes each value of  $U$  exactly twice as  $z_i$  and  $\epsilon_i$  run over the sets  $U$  and  $\{\xi, 1\}$  respectively. So  $M_{k,1} = 2^k (q-1)^k M_{k,2}$  where  $M_{k,2}$  counts the number of  $y_i \in \text{GF}(r)^*, z_i \in U \forall i$  such that

$$\sum_{i=1}^k y_i z_i^{jh} = 0, \forall 0 \leq j \leq t.$$

Similar to (16), the above equations can be solved completely by using a combinatorial method of [38]. We conclude that  $M_{k,2} = N_k$ , which is given by the formula (4). Interested readers may review [38] for details. Therefore we obtain  $M_k = (q-1)^k N_k$  as desired.

## 7.2 Case 2: $m$ and $h$ are both even

In this case  $r \equiv 1 \pmod{4}$ , we may take  $\xi = \gamma^{(r+1)/2}$ . Hence  $\xi^{(r-1)h} = 1$  as  $2|h$  and  $\xi^{r+1}$  is a non-square in  $\text{GF}(r)^*$ . So  $y_i^2 \epsilon_i^{r-1}$  takes each value of  $\text{GF}(r)^*$  exactly twice as  $y_i$  and  $\epsilon_i$  run over  $\text{GF}(r)^*$  and  $\{\xi, 1\}$ . Hence (24) can be reduced to

$$\sum_{i=1}^k \lambda_i \cdot y_i^f z_i^{-2jh} = 0, \forall 0 \leq j \leq t.$$

Since  $\left(f, \frac{r-1}{q-1}\right) = 1$ ,  $\lambda_i y_i^f$  will take each value of  $\text{GF}(r)^*$  exactly  $(q-1)$  times as  $\lambda_i$  and  $y_i$  run over  $\text{GF}(q)^*$  and  $\text{GF}(r)^*$  respectively. We have  $M_{k,1} = 2^k (q-1)^k M_{k,2}$ , where  $M_{k,2}$  is the number of solutions  $y_i \in \text{GF}(r)^*, z_i \in U \forall i$  such that

$$\sum_{i=1}^k y_i z_i^{-2jh} = 0, \forall 0 \leq j \leq t.$$

Again by using combinatorial argument as in [38] we can obtain that  $M_{k,2} = N_k$  for any  $1 \leq k \leq 2t$  which is given by (4). Hence we conclude  $M_k = (q-1)^k N_k$  as desired. This completes the proof of Lemma 8.  $\square$

Statement (ii) of Theorem 3 can be proved similarly by using the above idea and by modifying the proof of [38, Theorem 2] for  $\mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  accordingly. We omit the details.  $\square$

## 8 Conclusions

In this paper we extended [16, 38] further in two directions, that is, for any prime  $p$ ,  $q = p^l$  and  $r = q^m$ , we determined the weight distribution of the cyclic codes  $\mathcal{C}_{(d_0, d_1, \dots, d_t)}^{(1)}, \mathcal{C}_{(\tilde{d}_1, \dots, \tilde{d}_t)}^{(2)}$  over  $\text{GF}(q)$  whose duals have  $t+1$  and  $t$  generalized Niho type zeroes respectively for any  $t$  (see Theorems 1 and 3). Numerical examples show that the classes considered contain many optimal linear codes which were not presented in [16, 38].

## Acknowledgement

M. Xiong's research was supported by the Hong Kong Research Grants Council under Grant Nos. 609513 and 606211. N. Li's research was supported by the Norwegian Research Council.

## References

- [1] Y. AUBRY AND P. LANGEVIN, *On the weights of binary irreducible cyclic codes*, in Proceedings of the 2005 international conference on Coding and Cryptography, Springer-Verlag, LNCS, **3969** (2006), pp. 46-54.
- [2] L. D. BAUMERT AND R. J. MCELIECE, *Weights of irreducible cyclic codes*, Information and Control, **20** (1972), pp. 158-175.
- [3] L. D. BAUMERT AND J. MYKKELTVEIT, *Weight distributions of some irreducible cyclic codes*, DSN Progress Report, **16** (1973), pp. 128-131.
- [4] R. CALDERBANK AND W.M. KANTOR, *The geometry of two-weight codes*, Bull. Lond. Math. Soc., **18** (1986), pp. 97-122.
- [5] P. DELSARTE, *On subfield subcodes of modified Reed-Solomon codes*, IEEE Trans. Inform. Theory, **21** (1975), pp. 575-576.
- [6] C. DING, Y. LIU, C. MA AND L. ZENG, *The weight distributions of the duals of cyclic codes with two zeroes*, IEEE Trans. Inform. Theory, **57** (2011), pp. 8000-8006.
- [7] C. DING AND J. YANG, *Hamming weights in irreducible cyclic codes*, Discrete Mathematics, **313** (2013), pp. 434-446.
- [8] C. DING, Y. YANG, AND X. TANG, *Optimal sets of frequency hopping sequences from linear cyclic codes*, IEEE Trans. Inform. Theory, **56** (2010), pp. 3605-3612.
- [9] K. FENG AND J. LUO, *Weight distribution of some reducible cyclic codes*, Finite Fields Appl., **14** (2008), pp. 390-409.
- [10] T. FENG, *On cyclic codes of length  $2^r - 1$  with two zeroes whose dual codes have three weights*, Des. Codes Cryptogr., **62** (2012), pp. 253-258.
- [11] T. FENG AND K. MOMIHARA, *Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums*, IEEE Trans. Inform. Theory, **59** (2013), pp. 5980-5984.

- [12] R. FITZGERALD AND J. YUCAS, *Sums of Gauss sums and weights of irreducible codes*, Finite Fields Appl., **11** (2005), pp. 89-110.
- [13] H. D. L. HOLLMANN AND Q. XIANG, *On binary cyclic codes with few weights*, in Proc. Finite Fields Appl. (Augsburg), Berline, Germany, 1999, pp. 251-275.
- [14] T. KLØVE, *Codes for Error Detection*, Singapore: World Scientific, 2007.
- [15] S. LI, S. HU, T. FENG, AND G. GE, *The weight distribution of a class of cyclic codes related to Hermitian forms graphs*, IEEE Trans. Inform. Theory, **59** (2013), pp. 3064-3067.
- [16] S. LI, T. FENG, AND G. GE, *On the weight distribution of cyclic codes with Niho exponents*, IEEE Trans. Inform. Theory, **60** (2014), pp. 3903-3912.
- [17] J. LUO AND K. FENG, *On the weight distribution of two classes of cyclic codes*, IEEE Trans. Inform. Theory, **54** (2008), pp. 5332-5344.
- [18] J. LUO AND K. FENG, *Cyclic codes and sequences from generalized Coulter-Matthews function*, IEEE Trans. Inform. Theory, **54** (2008), pp. 5345-5353.
- [19] J. LUO, Y. TANG, AND H. WANG, *Cyclic codes and sequences: The generalized Kasami case*, IEEE Trans. Inform. Theory, **56** (2010), pp. 2130-2142.
- [20] C. MA, L. ZENG, Y. LIU, D. FENG AND C. DING, *The weight enumerator of a class of cyclic codes*, IEEE Trans. Inform. Theory, **57** (2011), pp. 397-402.
- [21] R. J. MCELIECE AND J. H. RUMSEY, *Euler products, cyclotomy, and coding*, J. Number Theory, **4** (1972), pp. 302-311.
- [22] M. MOISIO, *Explicit evaluation of some exponential sums*, Finite Fields Appl., **15** (2009), pp. 644-651.
- [23] M. MOISIO, K. RANTO, M. RINTAAHO, AND K. VÄÄNÄNEN, *On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeroes and hyper-Kloosterman codes*, Adv. Appl. Discrete Math. **3** (2009), pp. 155-164.
- [24] Y. NIHO, *Multivalued cross-correlation functions between two maximal linear recursive sequence*, Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1970.
- [25] A. RAO AND N. PINNAWALA, *A family of two-weight irreducible cyclic codes*, IEEE Trans. Inform. Theory, **56** (2010), pp. 2568-2570.
- [26] B. SCHMIDT AND C. WHITE, *All two-weight irreducible cyclic codes?*, Finite Fields Appl., **8** (2002), pp. 1-17.
- [27] R. SCHROOF, *Families of curves and weight distribution of codes*, Bull. Amer. Math. Soc., **32** (1995), 171-183.
- [28] A. THANGARAJ AND S. McLAUGHLIN, *Quantum codes from cyclic codes over  $GF(4^m)$* , IEEE Trans. Inform. Theory, **47** (2001), pp. 1176-1178.

- [29] M. VAN DER VLUGT, *Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes*, J. Number Theory, **55** (1995), pp. 145-159.
- [30] G. VEGA, *Determining the number of one-weight cyclic codes when length and dimension are given*, in Arithmetic of Finite Fields. Berlin, Germany: Springer, Lecture Notes Comput. Sci, **4547** (2007), pp. 284-293.
- [31] G. VEGA AND J. WOLFMANN, *New classes of 2-weight cyclic codes*, Des. Codes Cryptogr., **42** (2007), pp. 327-334.
- [32] G. VEGA, *The weight distribution of an extended class of reducible cyclic codes*, IEEE Trans. Inform. Theory, **58** (2012), pp. 4862-4869.
- [33] B. WANG, C. TANG, Y. QI, Y. YANG AND M. XU, *The weight distributions of cyclic codes and elliptic curves*, IEEE Trans. Inform. Theory, **58** (2012), pp. 7253-7259.
- [34] J. WOLFMANN, *Weight distributions of some binary primitive cyclic codes*, IEEE Trans. Inform. Theory, **40** (1994), pp. 2068-2071.
- [35] M. XIONG, *The weight distributions of a class of cyclic codes*, Finite Fields Appl., **18** (2012), pp. 933-945.
- [36] M. XIONG, *The weight distributions of a class of cyclic codes II*, Des. Codes Cryptogr., **72** (2014), pp. 511-528.
- [37] M. XIONG, *The weight distributions of a class of cyclic codes III*, Finite Fields Appl., **21** (2013), pp. 84-96.
- [38] M. XIONG, N. LI, Z. ZHOU AND C. DING, *Weight distribution of cyclic codes with arbitrary number of generalised Niho type zeroes*, to appear in Des. Codes Cryptogr.
- [39] J. YANG, M. XIONG, C. DING, AND J. LUO, *Weight distribution of a class of cyclic codes with arbitrary number of zeroes*, IEEE Trans. Inform. Theory, **59** (2013), pp. 5985-5993.
- [40] J. YANG, L. XIA, AND M. XIONG, *Weight distributions of a class of cyclic codes with arbitrary number of zeroes II*, CoRR abs/1405.6256, 2014.
- [41] X. ZENG, L. HU, W. JIANG, Q. YUE, AND X. CAO, *Weight distribution of a p-ary cyclic code*, Finite Fields Appl., **16** (2010), pp. 56-73.